NEW ORLEANS POLICE DEPARTMENT OPERATIONS MANUAL

CHAPTER: 82.3.6

TITLE: CRIMINAL HISTORY RECORD INFORMATION (CHRI)

EFFECTIVE: 12/17/2017
REVISED: Replaces Policy 812

PURPOSE

This Chapter provides guidelines for NOPD's access to state and federal databases related to Criminal History Record Information, as well as the security, maintenance and release of criminal records obtained through law enforcement telecommunications, terminals, and databases, including Criminal History Record Information (CHRI) (R.S. 15:578).

POLICY STATEMENT

1. The New Orleans Police Department will adhere to all state and federal laws, regulations of the Louisiana Bureau of Criminal Identification and Information related to the access, use and dissemination of sensitive information received via a law enforcement telecommunications network (R.S. 15:579).

DEFINITIONS:

Criminal History Record Information (CHRI)—Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, bills of information, or any formal criminal charges, and any disposition arising there from, including sentencing, correctional supervision, and release. This does not include intelligence or investigatory purposes, nor does it include any identification information which does not indicate involvement of the individual in the criminal justice system (R.S. 15:576(2)).

Network Terminal Agency Coordinator (TAC)—The FBI/NCIC requires that every law enforcement agency that utilizes NCIC designate one individual, who is employed by that agency, to function as NCIC Terminal Agency Coordinator (TAC). This person is responsible for ensuring compliance with NCIC policies and procedures. The person appointed as TAC is knowledgeable in all aspects of NCIC use and has the authority to implement changes and oversee operations, which affect the agency's use of NCIC.

RESPONSIBILITIES

2. The Custodian of Records, or his/her designee, shall appoint a Network Terminal Agency Coordinator who will serve as the liaison with the appropriate state agencies on matters pertaining to the security, access and use of information available via law

enforcement networks and databases.

3. It is the responsibility of the TAC to assist the Department in complying with all NCIC related laws and procedures.

DEPARTMENT MEMBER ACCESS

4. CHRI may be accessed or released as follows:
   (a) Members may access or otherwise obtain records or CHRI information and department files only in accordance with their official duties.
   (b) A member may not access confidential information until a background investigation has been completed on the member and approved and until he/she has completed all required training.
   (c) CHRI shall be used solely for the purpose for which it was obtained.
   (d) Members may not use CHRI information in any unauthorized manner, for any unauthorized purpose, or disclose CHRI to any person who is not entitled to the information.
   (e) Unauthorized access or release of information may subject the member to criminal prosecution.
   (f) Members violating this policy may also be subject to administrative action pursuant to the Personnel Complaints Policy.

RELEASE OF INFORMATION

5. Each person authorized to release CHRI information is responsible for ensuring that each request appears legitimate and that the requester is an authorized recipient.

6. Only the persons listed below are authorized to release CHRI information:
   (a) Terminal Agency Coordinator.
   (b) NOPD – NCIC Unit members.
   (c) Personnel specifically designated in writing by Superintendent of Police with the concurrence of the TAC.

AUTHORIZED RECIPIENTS

7. CHRI may be released to authorized NOPD members for criminal justice purposes.

8. All law enforcement personnel with proper identification are authorized recipients, if they are acting in the scope of their official duties.

9. Conviction records for certain crimes may be disseminated without restriction by authorized members (R.S. 15:548).

DISSEMINATION OF INFORMATION

10. When CHRI is disseminated, the NOPD – NCIC Unit shall maintain a dissemination log pertaining to each transaction with the appropriate information to include maintaining the log for the designated time period (R.S. 15:548(G).

PROTECTION OF INFORMATION

11. Sensitive information obtained through law enforcement databases, such as CHRI, should generally not be transmitted by radio.

12. Information shall be stored in the Records Division where constant personnel coverage

will be provided. If information is stored elsewhere for investigative or other law enforcement purposes, it shall be secured in locked desks, locked file cabinets or in locked rooms.

13. The Custodian of Records, or his/her designee, is responsible for necessary procedures to supervise and protect system information by (R.S. 15:589):
    (a) Limiting direct access to records.
    (b) Limiting direct access to information.
    (c) Including procedures to prevent file destruction.
    (d) Ensuring computer terminal security including preventing unauthorized access.
    (e) Utilizing a means of detection regarding unauthorized penetrations.
    (f) The proper destruction of records.
    (g) Designating where and how such records should be stored.

COMPUTER TERMINAL SECURITY

14. Computer terminal equipment that is capable of providing access to law enforcement databases, including automated CHRI records, shall be maintained in secure areas to preclude access by unauthorized individuals. The terminals must be housed in areas outside of screen view of the public at all times.

15. Officers shall ensure that patrol vehicles remain secured when unoccupied to preclude access to the Mobile Digital Computer (MDC) located within the vehicle that may have access to confidential information.

DESTRUCTION OF RECORDS

16. When any confidential document, including CHRI, has served the purpose for which it was obtained and is eligible for destruction, it should be disposed of via a permanent destruction method, in compliance with the organization's records retention schedule. At no time shall documents merely be placed in a trash receptacle.

17. Each member shall be responsible for properly destroying CHRI documents he/she receives.

REVIEW OF AND CHALLENGE TO RECORDS

18. The Department shall post a public notice informing individuals of their right to access and to administratively challenge the completeness or accuracy of their individual CHRI.

19. Every individual seeking to avail him/herself of this procedure shall be provided with a list of all affected agencies and informed of the significance of querying a non-affected agency.

20. If an individual seeks to review records not held by the Department, the individual should be directed to the applicable agency. Viewing of CHRI shall be limited to ordinary NOPD – NCIC Unit business hours.

REVIEW OF RECORDS

21. Upon written request and with proper payment of fees and proof of identification, an individual has the right to access and review his/her own CHRI on file with the Department. However, an individual is not entitled to data contained in intelligence, investigatory or other related files.

22. Individuals or their personal representatives seeking access shall be allowed to view the desired individual CHRI within a reasonable time, not to exceed three days, provided that where fingerprint classification is an essential prerequisite to the location and retrieval of the record sought, the time period within which viewing must be made possible may be extended by an additional 30 days.

23. The Department shall make available facilities and personnel necessary for such viewing and shall in all respects maintain a cooperative attitude toward individuals requesting viewing. Viewing shall occur only within department facilities and only under the supervision and in the presence of a designated member.

24. The Department shall, in every instance, diligently seek to provide the information requested. Every out-of-parish criminal justice agency listed on the request for viewing shall be contacted within seven days of receipt of the request for viewing.

25. When the Department receives a request for information, members must make every effort to locate the information requested and shall in any event forward a reply to the requesting agency within seven normal working days of receipt of the request, except as provided for requests to the central state repository.

26. The Department shall fingerprint individuals requesting that the central state repository be queried. In such instances where an authorized representative is presenting a query to the central state repository on behalf of an individual, the representative shall supply at least two sets of the represented individuals' fingerprints on standard fingerprint cards.

27. When CHRI is requested by a personal representative, the representative must present positive proof of the identity of the individual actually involved as well as a sworn authorization from the involved individual. Positive proof of identity shall mean fingerprints. Upon presentation on the authorization and positive identifier, the representative shall be permitted to request, examine, and/or challenge the CHRI specifically relating to the involved individual.

PRIVACY AND SECURITY OF REVIEW

28. A record of each individual viewing a record shall be maintained. Each viewing record shall be approved by the supervisory member present at the review. The reviewing individual shall be required to certify by his/her signature that he/she has viewed the CHRI requested.

CRIMINAL RECORDS CHECK INQUIRES

29. Due to the nature of ordinary police function, it is not always possible for an officer or other member to personally enter the inquiry transaction at a computer terminal. If the inquiring officer is unable to utilize a computer terminal, the following procedure shall be followed:
    (a) The officer or member actually entering the inquiry shall enter his social security number and password.
    (b) To relieve the person making the entry of responsibility for the retrieved information, he/she shall enter either the social security number or the car number of the individual requesting the information.
    (c) If the individual requesting the inquiry is not on duty, he/she shall supply his badge number to the member making the inquiry.
    (d) On all telephone inquiries, the requesting individual shall supply his/her social security number to the individual actually entering the data.

30. Members who fail to enter a social security number, car number or badge number of the member requesting information through the criminal records system shall be held responsible for the disposition of the information obtained through the computer check. The member shall also be subject to disciplinary action for failing to enter the required requestor information.

31. Members are reminded that information obtained through the criminal records system shall not be released to individuals outside the New Orleans Police Department without written permission of the Superintendent of Police, or his/her designee. An exception is granted to outside law enforcement personnel acting in the performance of their duty.

TRAINING

32. All personnel authorized to access, process or release information received from law enforcement telecommunications or databases shall be required to complete a training program prescribed by the commander of the NOPD – NCIC Unit. The Education & Training Division shall coordinate the course to provide training in the proper use, control, and dissemination of information.